WHAT IS CLAIMED IS:

1. An authentication communicating semiconductor device, comprising:

a semiconductor chip;

a main processing unit formed on said semiconductor chip for generating a key code according to a predetermined algorithm, for determining approval/non-approval of communication of data with an external device, and for controlling the communication;

an encryption unit formed on said semiconductor chip for encrypting and decoding communication data using the key code generated by said main processing unit;

a first interface unit formed on said semiconductor chip for conducting communication with an upper layer according to a predetermined protocol; and

a second interface unit formed on said semiconductor chip for conducting communication with a lower layer according to a predetermined protocol.

2. An authentication communicating semiconductor device according to claim 1, wherein said main processing unit comprises:

a nonvolatile memory having stored therein a program implementing a key generation algorithm and an authentication algorithm to authenticate an external device requesting data communication;

program-execution-type control means for generating a key code and for determining approval/non-

approval of communication of data with an external device according to the program; and

a volatile memory for providing a work area for said control means,

said nonvolatile memory, said control means, said volatile memory, said encryption unit, and said firs and second interface units being connected to each other via an internal bus.

3. An authentication communicating semiconductor device according to claim 2, wherein:

said encryption unit includes a register to which the key code generated by said main processing unit is set; and

said encryption unit encrypts and decodes communication data according to the key code set via said internal bus to said register.

4. An authentication communicating semiconductor device according to claim 3, wherein:

each of said first and second interface units includes a register to which a communication code is set; and

said each interface unit conducts communication according to a communication control code set by said main processing unit via said internal bus to said register.

5. An authentication communicating semiconductor device according to claim 4, further comprising an external terminal coupled with said internal bus.

6. An electronic device, comprising:

an authentication communicating semiconductor device according to claim 5; and

an external memory connected to said external terminal connect to said internal bus, wherein:

a communication control program includes setting of a communication path is stored in said external memory; and

said main processing unit sets according to said communication control program a communication code to said register of said each interface section to conduct communication with an external device.

7. An authentication communicating semiconductor device, comprising:

a single semiconductor chip;

an encryption unit formed on said single semiconductor chip for encrypting, in an encrypting mode, ordinary or non-encrypted statement data into encrypted statement data; for decoding, in a decoding mode, the encrypted statement data into ordinary statement data; and for directly passing data therethrough when neither encryption nor decoding is required;

a lower-layer interface unit formed on said single semiconductor chip for the encrypted statement data of said encryption unit for controlling a protocol of communication with a lower layer;

an upper-layer interface unit formed on said

single semiconductor chip for the ordinary statement data of said encryption unit for controlling a protocol of communication with an upper layer; and

a key generation unit formed on said single semiconductor chip for executing authentication processing of communication passing through the lower layer and for executing key generation processing for said encryption unit, wherein:

said lower-layer interface unit comprises at least one lower-layer communication path for communicating encrypted statement data with a lower-layer device controlling a communication signal outside said semiconductor chip;

said upper-layer interface unit comprises at least one upper-layer communication path for communicating ordinary statement data with an upper-layer device outside said semiconductor chip;

said key generation unit comprises a CPU, an ROM, and an RAM; and

said CPU sets a key register for said encryption unit to hold an encryption key, a control register of said lower-layer interface unit, and a control register of said upper-layer interface unit via a bus connecting said CPU, said encryption unit, said lower-layer interface unit, and said upper-layer interface unit to each other.

8. An authentication communicating semiconductor device according to claim 7, further comprising:

a first upper-layer-lower-layer communication path and a second upper-layer-lower-layer communication path between said lower-layer interface unit to said upper-layer interface unit without passing said encryption unit,

said upper-layer interface unit comprising a first upper-layer communication path and a second upper-layer communication path for communicating signals with an upper-layer device outside said semiconductor chip,

said first upper-layer communication path being capable of selecting data from said encryption unit and data from said lower-layer interface unit without passing through said encryption unit,

said second upper-layer communication path being capable of selecting data from said first upper-layer-lower-layer communication path and data from said second upper-layer-lower-layer communication path.

9. An authentication communicating semiconductor device according to claim 7, wherein:

said encryption unit comprises a first encryption circuit and a second encryption circuit; and

said upper-layer interface unit includes a first upper-layer interface unit and a second upper-layer interface unit,

said communication path of the ordinary statement data of said first encryption circuit being connected to said first upper-layer interface circuit,

said communication path of the ordinary statement data of said second encryption circuit being connected to said second upper-layer interface circuit,

said first upper-layer interface unit including a first upper-layer communication path for communicating signals with a first upper-layer device outside said semiconductor chip,

said second upper-layer interface unit including a second upper-layer communication path for communicating signals with a second upper-layer device outside said semiconductor chip.

10. An authentication communicating semiconductor device according to claim 8, further comprising an electrically rewritable nonvolatile memory formed on said semiconductor chip, said memory being connected to said internal bus.

11. An authentication communicating semiconductor device according to claim 7, wherein said lower-layer device is formed on said semiconductor chip, said authentication communicating semiconductor device further comprising at least one communication path for communicating signals with said lower-layer device.

12. An electronic device, comprising:

an authentication communicating semiconductor device according to one of claim 7;

said lower-layer device; and

a connector coupled with said lower-layer device, said connector being externally connectable to

a communication transmission medium.

13. An authentication communicating semiconductor device, comprising:

a semiconductor chip;

a main processing unit formed on said semiconductor chip for generating a key code according to a predetermined algorithm, for determining approval/non-approval of communication of data with an external device, and for controlling the communication;

an encryption unit formed on said semiconductor chip for encrypting and decoding communication data using the key code generated by said main processing unit; and

an interface unit formed on said semiconductor chip for conducting communication with an upper-layer or a lower-layer according to a predetermined protocol.